

Self-testing in parallel

Matthew McKague^{1,2}

¹Department of Computer Science, University of Otago

²Dodd-Walls Centre for Photonic and Quantum Technologies

E-mail: mckaguem@cs.otago.ac.nz

Abstract. Self-testing allows us to determine, through classical interaction only, whether some players in a non-local game share particular quantum states. Most work on self-testing has concentrated on developing tests for small states like one pair of maximally entangled qubits, or on tests where there is a separate player for each qubit, as in a graph state. Here we consider the case of testing many maximally entangled pairs of qubits shared between two players. Previously such a test was shown where testing is sequential, i.e., one pair is tested at a time. Here we consider the parallel case where all pairs are tested simultaneously, giving considerably more power to dishonest players. We derive sufficient conditions for a self-test for many maximally entangled pairs of qubits shared between two players and also two constructions for self-tests where all pairs are tested simultaneously.

1. Introduction

A non-local game is a scenario where two or more non-communicating players receive challenges or questions from a referee. The players respond to the referee who subsequently announces whether they have won the game. The possible questions and conditions for winning are publicly known. We are interested in the case where the players have quantum capabilities and may share entanglement, but where communication with the referee is classical. We will also concentrate on the case of two players, known as Alice and Bob.

Self-testing allows us to verify the functioning of quantum devices without reference to any trusted equipment. Two or more players are queried with classical strings and their classical outputs are observed. By checking these outputs we can, for some special cases, decide that the devices share a particular ideal state, and that they measure it according to some ideal operators (up to some equivalence). In the language of non-local games, self-testing means that for some non-local games there essentially exists only one strategy that obtains the maximal probability of winning. These results are also robust, allowing us to put error bounds on the state in the case of small amounts of noise in the devices. Indeed, the robustness of these results is essential for applications, since we can never measure the probability of winning exactly.

A natural and desirable extension to any self-test would be the ability to repeat it, allowing us to self-test many copies of the same state. This can be done quite naturally if the many copies are held in separate non-communicating devices. But what if we cannot guarantee separation of a large number of states? For example, we may wish to test a large number of pairs of maximally entangled qubits (each pair is known as one *e-bit*) where one qubit from each pair is held by Alice and the other qubit in each pair is held by Bob. Here we lose the very useful division of pairs into tensor products with each other. Instead we have the considerably weaker division into only two subsystems.

1.1. Parallel and sequential testing

There are two natural ways of performing a test many times over. The first is *sequential* testing, where each test is completed before the next test begins. For each test the referee will send the questions to the participants and wait for their responses before proceeding to the next test. In *parallel* testing, by contrast, all tests are in progress at the same time. Here the referee will send all questions for all tests to the participants at the same time and the participants will likewise send their answers for all tests together.

It is possible to make a sequential test into a parallel test by revealing all of the questions at once. We can also turn a parallel test into a sequential test by revealing the questions a piece at a time. In both cases, the parallel test allows for more strategies for the players because they have more information. Indeed, a sequential strategy can always be played as a parallel strategy, but the opposite is not always true. For us, this means that bounds that we place on strategies from parallel tests will also be valid for sequential tests.

In the strict sense, parallel testing would mean that we have many sub-tests, each of which is completely independent of the other sub-tests, i.e., there would be fresh independent randomness for each test and all possible combinations of questions for sub-tests could be asked. More generally, we might not have independent questions for each sub-test. We will develop a strictly parallel test and also a test which is not strictly parallel that requires fewer questions.

1.2. Previous work

Self-testing was introduced by Mayers and Yao in [MY04] where a test now known as the Mayers-Yao test was developed, with robustness bounds appearing in [MMMO06]. The CHSH test [CHSH69] is also known to be a self-test, a result which is implied in [PR92] with initial robustness results in [BLM⁺09]. Robustness results for the Mayers-Yao test and the CHSH test appear in [MYS12], which we use here. We will also use techniques from [McK13] which were originally developed for testing graph states.

The idea of using a self-test many times in parallel is used in [MMMO06], where the separate tests are assumed to be on separate subsystems. More recently, Reichardt et al. [RUV13] proved that sequential repetition of CHSH games can be used for self-testing. Wu et al. [WBMS15] consider the case of two CHSH games played in parallel.

1.3. Contributions

We make three main contributions in this paper. First we generalize the techniques used in [McK13] Theorem 3, allowing us to consider the case of only two players for testing multi-qubit states. We then use this to derive sufficient conditions for self-testing many e-bits shared between two players. The two-player multi-qubit result has independent value for self-testing, and is used in [WBMS15] to prove that the magic square game is a self-test.

The second contribution is to develop a test – based on the Mayers-Yao test for a single e-bit – that self-tests many e-bits. Interestingly, the test requires only a logarithmic number of measurements (in the number of e-bits tested), and has a robustness bound that scales linearly.

Our final contribution is to develop a self-test for many e-bits which is strictly parallel. The basic test is new, and can be seen as an extension of CHSH. This test has an exponential number of measurement settings, and the robustness also scales exponentially in the number of sub-tests. We also phrase this self-test as a non-local game, defining winning conditions for one round of the test, and give a robustness bound on how far away the strategy is from the ideal in terms of the winning probability.

2. Technical preliminaries

We define 1_k to be the n -bit string which is 1 in the k -th position and 0 everywhere else. For x an n -bit string, let $|x|$ be the number of 1's in x (the Hamming weight). Further, when n is even, define x_a to be the n -bit string that agrees with x for the first $\frac{n}{2}$ bits and is zero elsewhere. The n -bit string x_b agrees with x for the last $\frac{n}{2}$ bits and is zero elsewhere. Later, we will divide x between Alice and Bob so x_a represents x on Alice's side, and x_b is for Bob's side. The matrix R exchanges the first and second halves of a bit string. Since R simply applies a fixed permutation on the entries of a string, it preserves the dot product, so that $Rx \cdot Ry = x \cdot y$. Also, $R^2 = I$ so $Rx \cdot y = x \cdot Ry$.

We will be dealing with sums over all bit strings, for which the following lemma will be invaluable.

Lemma 1. *For s, t ranging over $\{0, 1\}^n$*

$$\frac{1}{2^n} \sum_s s \cdot t = \frac{|t|}{2} \tag{1}$$

$$\frac{1}{2^{2n}} \sum_{s,t} s \cdot t = \frac{n}{4} \tag{2}$$

$$\frac{1}{2^n} \sum_s (-1)^{s \cdot t} = \delta_{t,0} \tag{3}$$

The proofs of these equations are straightforward and left to the reader. Next we need to know something about how R behaves. This will later be used to simplify the phases in a graph state when R is the adjacency matrix. This corresponds to Lemma 2 in [McK13].

Lemma 2. *Let s and u be n -bit strings with n even. Then*

$$(R(s \oplus u) \cdot s) \oplus (R(s \oplus u)_a \cdot (s \oplus u)_b) = (Rs_b \cdot s_a) \oplus (Ru_a \cdot u_b) \quad (4)$$

Proof. Exploiting linearity and the fact that $x_a \cdot y_b = 0$ for any x, y we find

$$\begin{aligned} (R(s \oplus u) \cdot s) \oplus (R(s \oplus u)_a \cdot (s \oplus u)_b) = \\ (R(s \oplus u)_b \cdot s_a) \oplus (R(s \oplus u)_a \cdot s_b) \oplus \\ (R(s \oplus u)_a \cdot s_b) \oplus (R(s \oplus u)_a \cdot u_b). \end{aligned} \quad (5)$$

The centre two terms on the right side now cancel. Expanding once again we get

$$\begin{aligned} (R(s \oplus u) \cdot s) \oplus (R(s \oplus u)_a \cdot (s \oplus u)_b) = \\ (Rs_b \cdot s_a) \oplus (Ru_b \cdot s_a) \oplus (Rs_a \cdot u_b) \oplus (Ru_a \cdot u_b) \end{aligned} \quad (6)$$

Since R preserves the dot product the two middle terms cancel, leaving us with the desired result. \square

We will need a way to translate between inner products and the 2-norm.

Lemma 3. *Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be normalized states. If $|\langle\psi_1|\psi_2\rangle| \geq 1 - \epsilon$ for $\epsilon \geq 0$ then*

$$\| |\psi_1\rangle - |\psi_2\rangle \|_2 \leq \sqrt{2\epsilon} \quad (7)$$

The proof follows directly from the definition of $\|\cdot\|_2$. From now on, unless otherwise specified, $\|\cdot\| = \|\cdot\|_2$.

It is conventional to define a Pauli operator raised to a bit string by $P^t = \bigotimes_{k=1}^n P^{t_k}$. We will adopt a generalization of this notation. If we have operators $X_1 \dots X_n$ then for a bit string t we define

$$X^t := \prod_{k=1}^n X_k^{t_k}. \quad (8)$$

The order of the product is important since X_j may not commute with some other X_k . Hence we will make the convention that the index increases from left to right. When applied to a state this ordering means that the operators are applied to the state in order of decreasing index. With suitable modifications to the proof any other ordering will also work so long as it is kept consistent.

3. Testing with two players

In this section we develop the infrastructure necessary to test many e-bits using just two players. We divide this into two main parts. The first part, Lemma 4 – which is a generalization of [McK13] Theorem 3 – also applies to graph states and makes no assumptions about any type of tensor product structure or commutation between any operators. The change compared to [McK13] is to provide a slightly more streamlined proof with a better bound, and slightly different isometry that does not rely on commutation relations between subsystems.

The second part uses Lemma 4 to derive sufficient conditions for testing many e-bits. The two necessary bounds are derived in Lemma 5 and are analogous to the bounds given in [McK13] Corollary 1 and Lemma 4. There, however, a rich tensor-product structure was imposed by the division into many players, while here we have the much weaker structure provided by only two players. The challenge, then, is to use this weaker structure to obtain much the same results, albeit with weaker bounds. In Lemma 6 we use these bounds along with Lemma 4 to derive the sufficient conditions for testing many e-bits.

3.1. Sufficient conditions for self-testing graph states

Lemma 4. *Given an $n \times n$ $(0,1)$ -matrix \mathbf{A} and a function P such that for all $s, t \in \{0,1\}^n$*

$$P(s) + P(t) = P(s \oplus t) + s \cdot \mathbf{A}(s \oplus t) \pmod{2} \quad (9)$$

let $|\psi\rangle$ be the n -qubit state

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_u (-1)^{P(u)} |u\rangle. \quad (10)$$

Further suppose that $|\psi'\rangle \in \mathcal{H}$ is a normalized state, $\{X'_j\}_{j=1}^n, \{Z'_j\}_{j=1}^n$ are unitary, Hermitian operators on \mathcal{H} , and $\epsilon_{ac}(s, t) \geq 0$ and $\epsilon_{xz}(s) \geq 0$ are functions such that for any $s, t \in (0,1)^n$

$$\|X'^s Z'^t |\psi'\rangle - (-1)^{s \cdot t} Z'^t X'^s |\psi'\rangle\| \leq \epsilon_{ac}(s, t) \quad (11)$$

and

$$\|X'^s |\psi'\rangle - (-1)^{P(s)} Z'^{\mathbf{A}s} |\psi'\rangle\| \leq \epsilon_{xz}(s). \quad (12)$$

Then there exists an isometry Φ and a state $|junk\rangle$ such that for any $p, q \in (0,1)^n$

$$\begin{aligned} \|\Phi(X'^q Z'^p |\psi'\rangle) - |junk\rangle X^q Z^p |\psi\rangle\| \leq \\ \sqrt{\frac{1}{2^{2n-1}} \sum_{s,t} \epsilon_{ac}(s, p) + \epsilon_{ac}(s, p \oplus t) +} \\ \sqrt{\frac{1}{2^{2n-1}} \sum_{t,u} \epsilon_{ac}(t, u) + \epsilon_{xz}(u)}. \end{aligned} \quad (13)$$

Proof. We first specify the isometry Φ via a sequence of actions:

- (i) Attach $2n$ qubit ancillas with qubit k and $k+n$ in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ for each $k = 1 \dots n$.
- (ii) For $k = n \dots 1$ apply a controlled X'_k to $|\psi'\rangle$, controlled on ancilla qubit $k+n$.
- (iii) Apply Hadamard gates to the last n ancilla qubits
- (iv) For $k = n \dots 1$ apply a controlled Z'_k to $|\psi'\rangle$, controlled on ancilla qubit $k+n$.
- (v) Apply Hadamard gates to the last n ancilla qubits
- (vi) For $k = n \dots 1$ apply a controlled X'_k to $|\psi'\rangle$, controlled on ancilla qubit $k+n$.

The state after applying the isometry is straightforwardly found to be

$$|\psi_1\rangle = \Phi(X'^q Z'^p |\psi'\rangle) = \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{t \cdot (s \oplus u)} X'^u Z'^t X'^{s \oplus q} Z'^p |\psi'\rangle |su\rangle. \quad (14)$$

We will compare it to the following state:

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{t \cdot s + p \cdot (u \oplus s \oplus q) + P(u \oplus s \oplus q)} Z'^{t \oplus p \oplus \mathbf{A}(u \oplus s \oplus q)} |\psi'\rangle |su\rangle. \quad (15)$$

First, let us show that $|\psi_3\rangle$ is normalized.

$$\langle \psi_3 | \psi_3 \rangle = \frac{1}{2^{3n}} \sum_{s,t,t',u} (-1)^{(t \oplus t') \cdot s} \langle \psi' | Z'^{t \oplus t'} | \psi' \rangle \quad (16)$$

$$= \frac{1}{2^{2n}} \sum_{t,t'} \left(\sum_s (-1)^{(t \oplus t') \cdot s} \right) \langle \psi' | Z'^{t \oplus t'} | \psi' \rangle \quad (17)$$

$$= 1 \quad (18)$$

In the first line we omit s and u cross-terms which are zero from $\langle s'u' | su \rangle$ factors, and cancel common factors of Z' . There is also considerable cancellation in the phases. To obtain the second line, the summation over u becomes a factor of 2^n and we factor out the summation over s . By Lemma 1 this factor is 2^n when $t = t'$ and 0 otherwise, so all summands are in fact equal to 1.

With some work we can factor $|\psi_3\rangle$. First we make two changes of variable, $t \mapsto t \oplus p \oplus \mathbf{A}(s \oplus u)$, followed by $u \mapsto u \oplus q$. Then

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{s \cdot (t \oplus \mathbf{A}(s \oplus u)) + p \cdot u + P(u \oplus s)} Z'^t |\psi'\rangle |s\rangle |u \oplus q\rangle. \quad (19)$$

Applying (9), this becomes

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{s \cdot t + p \cdot u + P(u) + P(s)} Z'^t |\psi'\rangle |s\rangle |u \oplus q\rangle. \quad (20)$$

Now we can factor out the summation over u .

$$|\psi_3\rangle = \left(\frac{1}{\sqrt{2^{2n}}} \sum_{s,t} (-1)^{s \cdot t + P(s)} Z'^t |\psi'\rangle |s\rangle \right) \otimes \left(\sum_u (-1)^{p \cdot u + P(u)} |u \oplus q\rangle \right) \quad (21)$$

$$= \left(\frac{1}{\sqrt{2^{2n}}} \sum_{s,t} (-1)^{s \cdot t + P(s)} Z'^t |\psi'\rangle |s\rangle \right) \otimes X^q Z^p |\psi\rangle \quad (22)$$

Defining $|junk\rangle = \left(\frac{1}{\sqrt{2^{2n}}} \sum_{s,t} (-1)^{s \cdot t + P(s)} Z'^t |\psi'\rangle |s\rangle \right)$ we find that

$$|\psi_3\rangle = |junk\rangle X^q Z^p |\psi\rangle. \quad (23)$$

Now we wish to estimate the distance between $|\psi_1\rangle$ and $|\psi_3\rangle$. To do this we will use an intermediate step in the form of the state

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{t \cdot (u \oplus q)} X'^{tu \oplus s \oplus q} Z'^{t \oplus p} |\psi'\rangle |su\rangle. \quad (24)$$

First we estimate the distance between $|\psi_1\rangle$ and $|\psi_2\rangle$, which we will do by estimating the inner product:

$$\langle \psi_2 | \psi_1 \rangle = \frac{1}{2^{3n}} \sum_{s,t,t',u} (-1)^{t' \cdot (u \oplus q) + t \cdot (s \oplus u)} \langle \psi' | Z'^{t' \oplus p} X'^{tu \oplus s \oplus q} X'^u Z'^t X'^{s \oplus q} Z'^p | \psi' \rangle. \quad (25)$$

Here we have omitted many zero cross terms for u and s resulting from the factor $\langle su | s'u' \rangle$. Now we can do some cleaning up by the change of variable $s \mapsto s \oplus q$ and cancelling an X'^u factor. This further allows us to factor out the sum over u . We then do a further change of variable $u \mapsto u \oplus q$, giving

$$\langle \psi_2 | \psi_1 \rangle = \frac{1}{2^{3n}} \sum_{s,t,t'} \left(\sum_u (-1)^{u \cdot (t \oplus t')} \right) (-1)^{s \cdot t} \langle \psi' | Z'^{t' \oplus p} X'^{ts} Z'^t X'^s Z'^p | \psi' \rangle. \quad (26)$$

According to Lemma 1 we can set $t = t'$ since all other terms will be zero. Let us further make the substitution $\langle \psi' | Z'^{t' \oplus p} X'^{ts} Z'^t X'^s Z'^p | \psi' \rangle = (-1)^{s \cdot t} (1 - e(s, t, p))$, giving

$$\langle \psi_2 | \psi_1 \rangle = 1 - \frac{1}{2^{2n}} \sum_{s,t} e(s, t, p) \quad (27)$$

Two applications of (11) give us

$$\left| \langle Z'^t X'^s Z'^p | \psi' \rangle - (-1)^{s \cdot t} \langle X'^s Z'^{t \oplus p} | \psi' \rangle \right| \leq \epsilon_{ac}(s, p) + \epsilon_{ac}(s, p \oplus t). \quad (28)$$

Multiplying on the left by the norm-1 operator $\langle \psi' | Z'^{t \oplus p} X'^s$ allows us to bound $|e(s, t, p)| \leq \epsilon_{ac}(s, p) + \epsilon_{ac}(s, p \oplus t)$ and hence by Lemma 3

$$\| |\psi_1\rangle - |\psi_2\rangle \| \leq \sqrt{\frac{1}{2^{2n-1}} \sum_{s,t} \epsilon_{ac}(s, p) + \epsilon_{ac}(s, p \oplus t)} \quad (29)$$

Next we estimate the distance between $|\psi_2\rangle$ and $|\psi_3\rangle$. After dropping zero cross-terms for s and u we obtain

$$\langle \psi_2 | \psi_3 \rangle = \frac{1}{2^{3n}} \sum_{s,t,t',u} (-1)^{t' \cdot (u \oplus q) + t \cdot s + p \cdot (s \oplus u \oplus q) + P(u \oplus s \oplus q)} \langle \psi' | Z'^{t' \oplus p} X'^{tu \oplus s \oplus q} Z'^{t \oplus p \oplus \mathbf{A}(u \oplus s \oplus q)} | \psi' \rangle \quad (30)$$

We make changes of variable $u \mapsto s \oplus u \oplus q$ to clean things up, after which we can factor out the sum over s , giving

$$\langle \psi_2 | \psi_3 \rangle = \frac{1}{2^{3n}} \sum_{t,t',u} \left(\sum_s (-1)^{s \cdot (t' \oplus t)} \right) (-1)^{u \cdot (t' \oplus p) + P(u)} \langle \psi' | Z'^{t' \oplus p} X'^u Z'^{t \oplus p \oplus \mathbf{A}u} | \psi' \rangle \quad (31)$$

Applying Lemma 1, we can drop all terms except where $t = t'$. We further make the change of variable $t \mapsto t \oplus p$ and the substitution $\langle \psi' | Z^t X^u Z^{t \oplus \mathbf{A}u} | \psi' \rangle = (-1)^{u \cdot t + P(u)} (1 - f(t, u))$ to obtain

$$\langle \psi_2 | \psi_3 \rangle = 1 - \frac{1}{2^{2n}} \sum_{t,u} f(t, u). \quad (32)$$

We can estimate $f(t, u)$ by first using (11) and then (12) to find

$$\left| \langle X^u Z^t | \psi' \rangle - (-1)^{u \cdot t + P(u)} \langle Z^{t \oplus \mathbf{A}u} | \psi' \rangle \right| \leq \epsilon_{ac}(t, u) + \epsilon_{xz}(u). \quad (33)$$

Then multiplying on the left by the norm-1 operator $\langle \psi' | Z^t X^u$ gives us $f(t, u) \leq \epsilon_{ac}(t, u) + \epsilon_{xz}(u)$ and then by Lemma 3

$$\|\psi_2 - \psi_3\| \leq \sqrt{\frac{1}{2^{2n-1}} \sum_{t,u} \epsilon_{ac}(t, u) + \epsilon_{xz}(u)} \quad (34)$$

The triangle inequality allows us to estimate $\|\psi_1 - \psi_3\|$ and gives us our desired result. \square

The isometry and proof are very similar to that in [McK13], but there are some important differences. Here, we do not have any assumptions about whether the operators commute. This means that in general Φ cannot be factored into a tensor product, or even a product of commuting isometries. However, if some commutation relations are known between operators, it may be possible to factor Φ . The proof here is slightly rearranged, requiring only one intermediate step instead of three, and of course phrased for maximum generality.

Here we have in mind that the matrix \mathbf{A} is the adjacency matrix of some graph and $|\psi\rangle$ is the corresponding graph state. In this case, setting $P(s) = (\frac{1}{2}s \cdot \mathbf{A}s) \pmod{2}$ has the required property, as shown in [McK13] Lemma 2.

3.2. Sufficient conditions for self-testing many maximally entangled pairs of qubits

The goal of the following lemma is to reduce the conditions of Lemma 4 to something easier to deal with. In Lemma 4 we needed to consider products of up to n operators, but any one measurement will provide direct information about products of one operator on Alice's side and one on Bob's side. Thus we need to use the direct information from measurements to learn about the products required for Lemma 4.

Note that R is the adjacency matrix for $\frac{n}{2}$ isolated edges. The corresponding graph state is then $\frac{n}{2}$ maximally entangled pairs of qubits.

Lemma 5. *Suppose that*

- (i) $|\psi'\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a state
- (ii) $\{X'_k\}_{k=1}^{\frac{n}{2}}$ are unitary, Hermitian, pair-wise commuting operators on \mathcal{H}_A
- (iii) $\{Z'_k\}_{k=1}^{\frac{n}{2}}$ are unitary, Hermitian, pair-wise commuting operators on \mathcal{H}_A
- (iv) $\{X'_k\}_{k=\frac{n}{2}+1}^n$ are unitary, Hermitian, pair-wise commuting operators on \mathcal{H}_B

(v) $\{Z'_k\}_{k=\frac{n}{2}+1}^n$ are unitary, Hermitian, pair-wise commuting operators on \mathcal{H}_B such that for all $k \neq \ell$

$$\|X'_k Z'_\ell |\psi'\rangle - Z'_\ell X'_k |\psi'\rangle\| \leq \epsilon_1 \quad (35)$$

$$\|X'_k |\psi'\rangle - Z'_{k+\frac{n}{2}} |\psi'\rangle\| \leq \epsilon_2 \quad (36)$$

$$\|Z'_k X'_k |\psi'\rangle + X'_k Z'_k |\psi'\rangle\| \leq \epsilon_3 \quad (37)$$

where $k + \frac{n}{2}$ is taken modulo n . Then

(i) for any $s, t \in (0, 1)^{2n}$

$$\begin{aligned} & \|X'^s Z'^t |\psi'\rangle - (-1)^{s \cdot t} Z'^t X'^s |\psi'\rangle\| \leq \\ & (|s_a| |t_a| + |s_b| |t_b|) (\epsilon_1 + 2\epsilon_2) + \\ & (t \cdot s) (\epsilon_3 - \epsilon_1) + 2\epsilon_2 \min\{|s|, |t|\} =: \epsilon_{ac}(s, t) \end{aligned} \quad (38)$$

(ii) for any $s \in (0, 1)^{2n}$

$$\begin{aligned} & \|X'^s |\psi'\rangle - (-1)^{Rs_a \cdot s_b} Z'^{Rs} |\psi'\rangle\| \leq \\ & |s| \epsilon_2 + \epsilon_{ac}(s_a, Rs_b) + \epsilon_{ac}(s_b, Rs_a) =: \epsilon_{xz}(s). \end{aligned} \quad (39)$$

For (i) we need to use the anti-commutation and commutation estimate many times in order to exchange the position of the X' and Z' operators. For (ii) we additionally need to use the correlation estimates many times to change X' operators into Z' operators. However, we can only use the estimates if the operators in question are rightmost in the product of operators. Hence we must take advantage of the fact that many of the operators exactly commute to move two operators of interest to the right so we can apply an estimate. The ordering of these moves is quite sensitive. Before proving the lemma we will first need to prove the following claim which will help us with the reorderings:

Claim 1. Let $k \in \{1, \dots, n\}$ and $t \in \{0, 1\}^n$ such that either $k \leq \frac{n}{2}$ and $t = t_a$, or $k > \frac{n}{2}$ and $t = t_b$. Then under the conditions of Lemma 5

$$\|Z'^t X'_k |\psi'\rangle - (-1)^{t_k} X'_k Z'^t |\psi'\rangle\| \leq |t|(\epsilon_1 + 2\epsilon_2) + t_k(\epsilon_3 - \epsilon_1) \quad (40)$$

and

$$\|X'^t Z'_k |\psi'\rangle - (-1)^{t_k} Z'_k X'^t |\psi'\rangle\| \leq |t|(\epsilon_1 + 2\epsilon_2) + t_k(\epsilon_3 - \epsilon_1) \quad (41)$$

Proof. We will consider the case where $k \leq \frac{n}{2}$ and $t = t_a$. The other case follows analogously. The general idea will be to take advantage of the fact that all operators are on Alice's side. We can move a single operator to Bob's side using an estimation, after which it will freely commute past all other operators.

Begin by defining i_m to be the m th index ℓ such that $t_\ell = 1$. Thus

$$Z'^t = Z'_{i_1} \dots Z'_{i_{|t|}} \quad (42)$$

Note that $i_m \leq \frac{n}{2}$ for all m . For now, let us suppose that $t_k = 0$ so that i_m is never equal to k . We move X'_k to the left one position using (35):

$$\|Z'_{i_1} \dots Z'_{i_{|t|}} X'_k |\psi'\rangle - Z'_{i_1} \dots Z'_{i_{|t|-1}} X'_k Z'_{i_{|t|}} |\psi'\rangle\| \leq \epsilon_1 \quad (43)$$

Now $Z'_{i_{|t|}}$ can then be moved over to Bob's side using (36), giving

$$\left\| Z'_{i_1} \dots Z'_{i_{|t|}} X'_k |\psi'\rangle - Z'_{i_1} \dots Z'_{i_{|t|-1}} X'_k X'_{i_{|t|} + \frac{n}{2}} |\psi'\rangle \right\| \leq \epsilon_1 + \epsilon_2. \quad (44)$$

We can now move $X'_{i_{|t|} + \frac{n}{2}}$ all the way to the left since all other operators are on Alice's subsystem. We repeat the above sequence $|t|$ times for each Z'_{i_j} , resulting in

$$\left\| Z'_{i_1} \dots Z'_{i_{|t|}} X'_k |\psi'\rangle - X'_{i_{|t|} + \frac{n}{2}} \dots X'_{i_1 + \frac{n}{2}} X'_k |\psi'\rangle \right\| \leq |t|(\epsilon_1 + \epsilon_2). \quad (45)$$

X'_k moves to the left past all other operators, since it is the only operator left on Alice's system.

$$\left\| Z'_{i_1} \dots Z'_{i_{|t|}} X'_k |\psi'\rangle - X'_k X'_{i_{|t|} + \frac{n}{2}} \dots X'_{i_1 + \frac{n}{2}} |\psi'\rangle \right\| \leq |t|(\epsilon_1 + \epsilon_2). \quad (46)$$

One by one, we transfer each X' on Bob's system operator back to a Z' on Alice's system and move it to the left. This gives

$$\left\| Z'_{i_1} \dots Z'_{i_{|t|}} X'_k |\psi'\rangle - X'_k Z'_{i_1} \dots Z'_{i_{|t|}} |\psi'\rangle \right\| \leq |t|(\epsilon_1 + 2\epsilon_2) \quad (47)$$

If $t_k = 1$, then we must make an adjustment: when $i_m = k$ we must swap positions of X'_k and Z'_k using (37) instead of (35). The result is a phase of -1 , and an error of ϵ_3 instead of ϵ_1 , giving

$$\left\| Z'_{i_1} \dots Z'_{i_{|t|}} X'_k |\psi'\rangle + X'_k Z'_{i_1} \dots Z'_{i_{|t|}} |\psi'\rangle \right\| \leq |t|(\epsilon_1 + 2\epsilon_2) + \epsilon_3 - \epsilon_1. \quad (48)$$

Combining the two cases above gives (40). Noting that the conditions of the lemma are symmetric in the roles of X and Z , we can run the entire argument again with X and Z swapped to obtain (41). \square

Proof of Lemma 5. Noting that X'^{s_a} and Z'^{t_a} are operators on Alice's system while X'^{s_b} and Z'^{t_b} are on Bob's system,

$$X'^{s_a} Z'^{t_a} = X'^{s_b} Z'^{t_b} X'^{s_a} Z'^{t_a}. \quad (49)$$

Let $k \in \{1 \dots n\}$ be the smallest such that $(s_a)_k = 1$. We apply Claim 1 to obtain

$$\left\| X'^{s_a} Z'^{t_a} |\psi'\rangle - (-1)^{t_k} X'^{s_b} Z'^{t_b} X'^{s_a \oplus 1_k} Z'^{t_a} X'_k |\psi'\rangle \right\| \leq |t_a|(\epsilon_1 + 2\epsilon_2) + t_k(\epsilon_3 - \epsilon_1). \quad (50)$$

Next we apply (35) to move X'_k to $Z'_{k + \frac{n}{2}}$ on Bob's side, which is then commuted to the left, giving

$$\left\| X'^{s_a} Z'^{t_a} |\psi'\rangle - (-1)^{t_k} X'^{s_b} Z'^{t_b} Z'_{k + \frac{n}{2}} X'^{s_a \oplus 1_k} Z'^{t_a} |\psi'\rangle \right\| \leq |t_a|(\epsilon_1 + 2\epsilon_2) + t_k(\epsilon_3 - \epsilon_1) + \epsilon_2. \quad (51)$$

Repeating this for each position where $s_a = 1$ we get

$$\left\| X'^{s_a} Z'^{t_a} |\psi'\rangle - (-1)^{t_a \cdot s_a} X'^{s_b} Z'^{t_b} Z'^{R s_a} Z'^{t_a} |\psi'\rangle \right\| \leq |s_a| |t_a| (\epsilon_1 + 2\epsilon_2) + (t_a \cdot s_a) (\epsilon_3 - \epsilon_1) + |s_a| \epsilon_2 \quad (52)$$

We can commute Z'^{Rs_a} past Z'^{t_a} since they are on different systems, and then apply (35) $|s_a|$ more times. Finally, we commute all the operators on Alice's side to the left past Bob's operators to obtain

$$\begin{aligned} \left\| X'^s Z'^t |\psi'\rangle - (-1)^{t_a \cdot s_a} Z'^{t_a} X'^{s_a} X'^{s_b} Z'^{t_b} |\psi'\rangle \right\| \leq \\ |s_a| |t_a| (\epsilon_1 + 2\epsilon_2) + (t_a \cdot s_a) (\epsilon_3 - \epsilon_1) + 2|s_a| \epsilon_2. \end{aligned} \quad (53)$$

Applying the whole procedure again, swapping the roles of Alice and Bob, we find

$$\begin{aligned} \left\| X'^s Z'^t |\psi'\rangle - (-1)^{s \cdot t} Z'^t X'^s |\psi'\rangle \right\| \leq \\ (|s_a| |t_a| + |s_b| |t_b|) (\epsilon_1 + 2\epsilon_2) + (t \cdot s) (\epsilon_3 - \epsilon_1) + 2|s| \epsilon_2. \end{aligned} \quad (54)$$

Since the conditions of the lemma are symmetric in the roles of X and Z , we can obtain a similar result with error bounded by $(|s_a| |t_a| + |s_b| |t_b|) (\epsilon_1 + 2\epsilon_2) + (t \cdot s) (\epsilon_3 - \epsilon_1) + 2|t| \epsilon_2$ instead. Taking the minimum we obtain (38).

Now we turn our attention to part ii. Let $k \in \{1 \dots \frac{n}{2}\}$ be the first index such that $s_k = 1$. Initially, X'_k commutes past everything to the right. Then we can apply (36) to obtain

$$\left\| X'^s |\psi'\rangle - X'^{s \oplus 1_k} Z'_{k+\frac{n}{2}} |\psi'\rangle \right\| \leq \epsilon_2. \quad (55)$$

Applying this in turn for each k such that $(s_a)_k = 1$, we find

$$\left\| X'^s |\psi'\rangle - X'^{s_b} Z'^{Rs_a} |\psi'\rangle \right\| \leq |s_a| \epsilon_2. \quad (56)$$

At this point we have a problem, since the remaining X'_k are on Bob's side, along with all of the Z' . Applying (38), however, we find

$$\left\| X'^s |\psi'\rangle - (-1)^{Rs_a \cdot s_b} Z'^{Rs_a} X'^{s_b} |\psi'\rangle \right\| \leq |s_a| \epsilon_2 + \epsilon_{ac}(s_a, Rs_b). \quad (57)$$

Now we can continue to turn X'_k into $Z'_{k+\frac{n}{2}}$ for the remaining k such that $(s_b)_k = 1$. The final result is

$$\left\| X'^s |\psi'\rangle - (-1)^{Rs_a \cdot s_b} Z'^{Rs} |\psi'\rangle \right\| \leq |s| \epsilon_2 + \epsilon_{ac}(s_a, Rs_b) + \epsilon_{ac}(s_b, Rs_a) \quad (58)$$

□

Now we are ready to combine Lemmas 4 and 5 to prove sufficient conditions for self-testing many maximally entangled pairs of qubits.

Lemma 6. *Under the conditions of Lemma 5 there exists an isometry Φ and a state $|junk\rangle$ such that for any $p, q \in (0, 1)^n$*

$$\begin{aligned} \left\| \Phi(X'^q Z'^p |\psi'\rangle) - |junk\rangle X^q Z^p |\psi\rangle \right\| \leq \\ \sqrt{\frac{|p|}{2} ((n-1)\epsilon_1 + 2n\epsilon_2 + \epsilon_3) + \frac{n}{4} (\epsilon_3 - \epsilon_1) + \frac{n^2}{8} (\epsilon_1 + 2\epsilon_2) +} \\ \sqrt{\frac{n^2}{4} (\epsilon_1 + 2\epsilon_2) + \frac{n}{2} (\epsilon_2 + \epsilon_3 - \epsilon_1)}. \end{aligned} \quad (59)$$

Proof. The conditions of Lemma 5, together with Lemma 2 straightforwardly imply the conditions of Lemma 4. All that remains is to substitute in the error estimates to calculate the bound. This is done using Lemma 1 repeatedly. \square

4. Parallelizing the Mayers-Yao test

We want to test $\frac{n}{2}$ e-bits shared between Alice and Bob, so we will devise some test that allows us, for honest players, to fulfill the conditions of Lemma 6. This test will be based on the Mayers-Yao test for a single e-bit.

Let us first summarize the conditions of Lemma 6. We need some X' operators on Alice's system that commute with each other, and similar for Bob. We also need some Z' operators that commute with each other for Alice and some more for Bob. These are easy enough to construct, and the commutation properties will follow directly from the construction. Next we need Alice's X'_j measurements to correlate with Bob's Z'_j measurements, which we can test by asking Alice and Bob to perform those measurements and checking their answers. We also need Alice's X'_j measurement to anti-commute with her Z'_j measurement. This is established using measurements from the Mayers-Yao test.

So far, everything is very similar to other self-tests (such as [MYS12] and [McK11]), in which the most difficult part is to show that we have anti-commuting operators. Indeed, the conditions outlined so far are sufficient to show that there is at least *one* maximally entangled pair of qubits. However, we do not yet have any way of guaranteeing that Alice's system j is independent of her system k (for $j \neq k$), so there might be *only* one pair. Here we will guarantee independence by the fact that Alice's X'_j commutes with Z'_k for $j \neq k$. Interestingly, this will be in some sense the most difficult part, with all but a constant number of measurement settings being dedicated to establishing this property. While in [MYS12] and [McK11] we need to add measurements to show that some things anti-commute, here we add measurements to show that some things commute.

4.1. Structure of test and honest behaviour

It will be convenient to specify both the structure of the test and the honest behaviour together. Alice and Bob will start off sharing the following state, which is the graph state of $\frac{n}{2}$ isolated edges:

$$|\psi\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle - |11\rangle)^{\otimes \frac{n}{2}}. \quad (60)$$

Here Alice holds the first qubit of each pair, and Bob holds the second, so that Alice's qubit k is entangled with Bob's qubit k .

The possible questions (measurement settings) for Alice are:

A_X Alice measures each of her $\frac{n}{2}$ qubits in the eigenbasis of X and returns the results.

A_Z Alice measures each of her $\frac{n}{2}$ qubits in the eigenbasis of Z and returns the results.

- A_D Alice measures each of her $\frac{n}{2}$ qubits in the eigenbasis of $D = \frac{X+Z}{\sqrt{2}}$ and returns the results.
- A_{X_j} For each $k = 1 \dots \frac{n}{2}$, Alice measures her k th qubit in basis X if the j th bit of k (as a binary number) is 1. Otherwise she measures in basis Z . She returns the results.
- A_{Z_j} For each $k = 1 \dots \frac{n}{2}$, Alice measures her k th qubit in basis Z if the j th bit of k is 0. Otherwise she measures in basis X . She returns the results.

Bob's questions and behaviour are analogous. For our convenience, the players will return their measurement results as the eigenvalue, i.e., ± 1 .

The referee will never choose the question $A_D B_D$ or any combination of A^{X_j} or A^{Z_j} with B^{X_ℓ} or B^{Z_ℓ} since we will not use any of these measurements.

4.2. General behaviour

Each player receives one question and returns $\frac{n}{2}$ answers as a string in $\{-1, 1\}^{\frac{n}{2}}$. The most general behaviour for the players to share some joint state $|\psi'\rangle$ and each player performs a POVM on their subsystem and returns the result. Since we are not concerned with the dimension of the players' systems, we can perform a Steinspring dilation and turn the POVM into a projective measurement. Note that the dilation is an isometry on the player's system, and so it can be absorbed into our definition of Φ (the composition of two isometries is again an isometry). Also, if the state is mixed we can include the purification in the state, so it is not a restriction to assume that it is pure.[‡]

Now a player's behaviour can be modelled as a collection of projective measurements:

$$\mathcal{M}_q = \{\Pi_a^q\}_a \quad (61)$$

where q is the question, a is a string of answers and $\Pi_a^q \Pi_b^q = \delta_{a,b} \Pi_a^q$. We can define projectors for individual symbols in the answer as follows:

$$\Gamma_{k,x}^q = \sum_{a: a_k=x} \Pi_a^q \quad (62)$$

where $k \in \{1 \dots \frac{n}{2}\}$, a_k is the k -th symbol of a , and $x = \pm 1$. Note that for all j, k, x, y the operators $\Gamma_{j,x}^q$ and $\Gamma_{k,y}^q$ commute since Π_a^q and Π_b^q commute for all a, b . We can next define observables for each answer symbol as

$$M_k'^q = \Gamma_{k,1}^q - \Gamma_{k,-1}^q. \quad (63)$$

Note that $M_k'^q$ and $M_\ell'^r$ will commute whenever $q = r$ (by construction), or when q is a question for Alice and r is a question for Bob (since the operators are defined on two different subsystems). Now measuring \mathcal{M}_q is equivalent to measuring $M_k'^q$ for each k and returning the resulting eigenvalues as a string. Each $M_k'^q$ is Hermitian and unitary.

[‡] Another way of dealing with mixed states is to introduce a third register to hold the purification. Then Alice and Bob's measurements will never touch the purification. From the construction it is obvious that Φ will never touch this third register, nor will the operators obtained by applying Φ to Alice and Bob's measurements. We can then know for sure that the purification register ends up in $|junk\rangle$ and that no part of the self-tested state resides in the purification.

We will give some more convenient names for some of these operators.

$$X'_k = M'_k{}^X \begin{cases} M'_k{}^{AX} & 0 < k \leq \frac{n}{2} \\ M'_{k-\frac{n}{2}}{}^{BX} & \frac{n}{2} < k \leq n \end{cases} \quad (64)$$

$$Z'_k = M'_k{}^Z \begin{cases} M'_k{}^{AZ} & 0 < k \leq \frac{n}{2} \\ M'_{k-\frac{n}{2}}{}^{BZ} & \frac{n}{2} < k \leq n \end{cases} \quad (65)$$

$$M'_k{}^{Xj} = \begin{cases} M'_k{}^{AXj} & 0 < k \leq \frac{n}{2} \\ M'_{k-\frac{n}{2}}{}^{BXj} & \frac{n}{2} < k \leq n \end{cases} \quad (66)$$

$$M'_k{}^{Zj} = \begin{cases} M'_k{}^{AZj} & 0 < k \leq \frac{n}{2} \\ M'_{k-\frac{n}{2}}{}^{BZj} & \frac{n}{2} < k \leq n \end{cases} \quad (67)$$

For convenience we will also define operators M_k^{Xj} etc. (i.e., without the \prime) for the honest behaviour, which will be one of the Pauli operators X or Z , or the sum $\frac{X+Z}{\sqrt{2}}$.

4.3. Proof of self-testing

Lemma 7. *Given the definitions of operators in section 4.2,*

(i) *for all k, ℓ*

$$X'_\ell X'_k = X'_k X'_\ell \quad (68)$$

$$Z'_\ell Z'_k = Z'_k Z'_\ell \quad (69)$$

(ii) *when $k \leq \frac{n}{2}, \ell > \frac{n}{2}$ or $\ell \leq \frac{n}{2}, k > \frac{n}{2}$*

$$X'_\ell Z'_k = Z'_k X'_\ell \quad (70)$$

If additionally for each $q, r \in \{X, Z\} \cup \{X_j\}_j \cup \{Z_j\}_j$ and $0 < k \leq \frac{n}{2}$ we have

$$\left| \langle \psi' | M_k'^q M_{k+\frac{n}{2}}'^r | \psi' \rangle - \langle \psi | M_k^q M_{k+\frac{n}{2}}^r | \psi \rangle \right| \leq \epsilon \quad (71)$$

then

(iii) *for all k*

$$\left\| X'_k | \psi' \rangle - Z'_{k+\frac{n}{2}} | \psi' \rangle \right\| \leq \sqrt{2\epsilon} \quad (72)$$

(where $k + \frac{n}{2}$ is taken modulo $2n$)

(iv) *for $k \neq \ell$ and $k, \ell \leq \frac{n}{2}$ or $k, \ell > \frac{n}{2}$*

$$\| X'_\ell Z'_k | \psi' \rangle - Z'_k X'_\ell | \psi' \rangle \| \leq 4\sqrt{2\epsilon} \quad (73)$$

Proof. Equations (68) and (69) follow directly from the construction of X'_j and Z'_j . For (70), if one of k and ℓ is less than or equal to $\frac{n}{2}$, and the other is greater than $\frac{n}{2}$, then X'_ℓ and Z'_k are on different subsystems, so they necessarily commute.

For (72), suppose $k \leq \frac{n}{2}$, with the other case following analogously. The honest behaviour for Alice is to measure her k th qubit in the X basis. Bob's honest behaviour is to measure his k th qubit in the Z basis. Hence

$$\langle \psi | X_k Z_{k+\frac{n}{2}} | \psi \rangle = 1 \quad (74)$$

and by assumption we then have

$$\langle \psi' | X'_k Z'_{k+\frac{n}{2}} | \psi' \rangle \geq 1 - \epsilon. \quad (75)$$

This readily translates into (72) using Lemma 3.

We now consider (73). Let us suppose that $k, \ell \leq \frac{n}{2}$. The other case follows analogously. We begin by looking at the binary representation of the numbers k and ℓ . Since $k \neq \ell$ there is some position j where their binary representations disagree. Let us suppose that the j th bit of k is 0 and the j th bit of ℓ is 1, with the other case following analogously. Consider the measurement $Z'_k M'^{Xj}_{k+\frac{n}{2}}$. In the honest case Alice would measure Z on her k th qubit, and Bob would measure X on his k th qubit, giving $\langle \psi | Z_k M'^{Xj}_{k+\frac{n}{2}} | \psi \rangle = 1$. Following the argument for (72) we find

$$\left\| M'^{Xj}_{k+\frac{n}{2}} | \psi' \rangle - Z'_k | \psi' \rangle \right\| \leq \sqrt{2\epsilon}. \quad (76)$$

Following an analogous argument, we determine that

$$\left\| M'^{Xj}_{\ell+\frac{n}{2}} | \psi' \rangle - X'_\ell | \psi' \rangle \right\| \leq 2\sqrt{2\epsilon}. \quad (77)$$

It is now straightforward to verify

$$\begin{aligned} \left\| X'_\ell Z'_k | \psi' \rangle - X'_\ell M'^{Xj}_{k+\frac{n}{2}} | \psi' \rangle \right\| &\leq \sqrt{2\epsilon} \\ \left\| X'_\ell Z'_k | \psi' \rangle - M'^{Xj}_{k+\frac{n}{2}} X'_\ell | \psi' \rangle \right\| &\leq \sqrt{2\epsilon} \\ \left\| X'_\ell Z'_k | \psi' \rangle - M'^{Xj}_{k+\frac{n}{2}} M'^{Xj}_{\ell+\frac{n}{2}} | \psi' \rangle \right\| &\leq 2\sqrt{2\epsilon} \\ \left\| X'_\ell Z'_k | \psi' \rangle - M'^{Xj}_{\ell+\frac{n}{2}} M'^{Xj}_{k+\frac{n}{2}} | \psi' \rangle \right\| &\leq 2\sqrt{2\epsilon} \\ \left\| X'_\ell Z'_k | \psi' \rangle - M'^{Xj}_{\ell+\frac{n}{2}} Z'_k | \psi' \rangle \right\| &\leq 3\sqrt{2\epsilon} \\ \left\| X'_\ell Z'_k | \psi' \rangle - Z'_k M'^{Xj}_{\ell+\frac{n}{2}} | \psi' \rangle \right\| &\leq 3\sqrt{2\epsilon} \\ \left\| X'_\ell Z'_k | \psi' \rangle - Z'_k X'_\ell | \psi' \rangle \right\| &\leq 4\sqrt{2\epsilon} \end{aligned}$$

On the second line we have used the fact that $M'^{Xj}_{k+\frac{n}{2}}$ is defined on Bob's subsystem, whereas X'_ℓ is on Alice's subsystem. The sixth line is analogous. On the fourth line, we have used the fact that $M'^{Xj}_{\ell+\frac{n}{2}}$ and $M'^{Xj}_{k+\frac{n}{2}}$ commute by construction, and the last line is (73) as desired. \square

Next we need to show that the X 's and Z 's anti-commute on the same sub-test. For this we will appeal to [MYS12] Theorem 3, which we summarize here.

Lemma 8 (McKague et al. [MYS12]). *Given a bipartite state $|\psi'\rangle$ and operators M'_A and N'_B with M, N ranging over $\{D, X, Z\}$, if we have for all M, N (excluding the case $M = D = N$)*

$$|\langle\psi'|M'_A N'_B|\psi'\rangle - \langle\psi|M_A N_B|\psi\rangle| \leq \epsilon \quad (78)$$

where $|\psi\rangle$ is the graph state of an isolated edge and A and B refer to different subsystems, then

$$\|Z'_A X'_A |\psi'\rangle + X'_A Z'_A |\psi'\rangle\| \leq 4 \left(1 + \sqrt{2}\right) (2\epsilon)^{\frac{1}{4}} + 8\sqrt{2}\epsilon + \left(5 + 3\sqrt{2}\right) (2\epsilon)^{\frac{3}{4}} \quad (79)$$

and analogously for the B side.

We are now ready to prove the main result, that our parallellized Mayers-Yao test is in fact a self-test.

Theorem 1. *Given the definitions of operators in section 4.2 if for each $q, r \in \{X, Z\} \cup \{X_j\}_j \cup \{Z_j\}_j$ and $0 < k \leq \frac{n}{2}$ we have*

$$\left| \langle\psi'|M_k'^q M_{k+\frac{n}{2}}'^r |\psi'\rangle - \langle\psi|M_k^q M_{k+\frac{n}{2}}^r |\psi\rangle \right| \leq \epsilon \quad (80)$$

then there exists an isometry Φ and a state $|junk\rangle$ such that for any $p, q \in (0, 1)^n$

$$\begin{aligned} \|\Phi(X'^q Z'^p |\psi'\rangle) - |junk\rangle X^q Z^p |\psi\rangle\| &\leq \sqrt{\sqrt{2}\epsilon \left(\frac{9n^2}{4} + \frac{3n}{2} \right) + \frac{n\epsilon_4}{2}} + \\ &\sqrt{\sqrt{2}\epsilon \left[\frac{9n^2}{8} + n \left(\frac{5|p|}{2} - \frac{1}{4} \right) - \frac{|p|}{2} \right] + \epsilon_4 \left(\frac{n}{4} + \frac{|p|}{2} \right)}. \end{aligned}$$

where

$$\epsilon_4 := 4 \left(1 + \sqrt{2}\right) (2\epsilon)^{\frac{1}{4}} + 8\sqrt{2}\epsilon + \left(5 + 3\sqrt{2}\right) (2\epsilon)^{\frac{3}{4}} \quad (81)$$

Proof. The conditions of the theorem allow us to use Lemma 7 to get most of the conditions for Lemma 6. Then for each $k = 1 \dots \frac{n}{2}$ we set $X'_A = X'_k$, $X'_B = X'_{k+\frac{n}{2}}$, and similar for Z and D . With these definitions, the conditions of the theorem give us the conditions for Lemma 8, and we can conclude that equation (37) in the conditions of Lemma 6 holds for k and $k + \frac{n}{2}$. Now we have all the conditions for Lemma 6, which gives us Φ and $|junk\rangle$. Substituting in for the ϵ 's gets us the final bound. \square

Although we have concentrated on a very small number of questions, it is a subset of the questions that would be asked in a strictly parallel version of the Mayers-Yao test. So a strictly parallel version of Mayers-Yao also self-tests many e-bits. However it is very inefficient since we ignore almost all of the questions that are asked.

5. A strictly parallel test

The parallel Mayers-Yao test developed in the previous section has some interesting properties, but it would be interesting to see how a strictly parallel test can be constructed. We will do so using a non-local game which incorporates aspects of both the Mayers-Yao and CHSH self-tests which makes it particularly suited to constructing a self-testing non-local game.

5.1. Structure of the test and honest behaviour

First we specify the test and honest behaviour for a single e-bit. Alice and Bob share the state $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$.

A_X Alice measures her qubit in the X eigenbasis.

A_Z Alice measures her qubit in the Z eigenbasis.

A_D Alice measures her qubit in the $\frac{X+Z}{\sqrt{2}}$ eigenbasis.

A_E Alice measures her qubit in the $\frac{X-Z}{\sqrt{2}}$ eigenbasis.

Bob's behaviour is analogous.

The referee will choose one question for Alice and one for Bob and send them. However, the referee will never choose the question pairs $A_X B_X$, $A_Z B_Z$, $A_D B_D$, $A_E B_D$, $A_D B_E$ or $A_E B_E$ since we not need them. There are thus 10 possible question pairs. Alice and Bob will return their measurement result as either ± 1 .

For the parallel version, testing $\frac{n}{2}$ e-bits, the referee chooses $\frac{n}{2}$ questions for Alice and Bob, one for each e-bit, chosen from the questions for the single copy. That is to say, the referee generates $\frac{n}{2}$ pairs of questions independently as specified for the single copy test. There are thus $10^{\frac{n}{2}}$ possible questions. Honest Alice and Bob measure all of their qubits in the appropriate bases depending on the questions as specified for the single copy and return the results as strings in $\{-1, 1\}^{\frac{n}{2}}$.

Note that there are an exponential number of possible questions, which is necessarily the case for any strictly parallel test.

5.2. General behaviour

Alice and Bob will hold some bipartite state $|\psi'\rangle$. Their measurements can be treated as in section 4.2 so that we have operators M_k^q for question q , sub-test number k . Since this test is strictly parallel, it makes sense to think of the questions as strings of questions. So, for example, we have question $A_{X\dots X}$ in which Alice is asked to measure X for each sub-test. We define:

$$M_k'^{S_1\dots S_n} = \begin{cases} M_k'^{A_{S_1\dots S_{\frac{n}{2}}}} & 0 < k \leq \frac{n}{2} \\ M_{k-\frac{n}{2}}'^{B_{S_{\frac{n}{2}+1}\dots S_n}} & \frac{n}{2} < k \leq n \end{cases} \quad (82)$$

$$X_k' = M_k'^{X\dots X} \quad (83)$$

$$Z_k' = M_k'^{Z\dots Z} \quad (84)$$

$$D_k' = M_k'^{D\dots D} \quad (85)$$

$$E_k' = M_k'^{E\dots E}. \quad (86)$$

5.3. Proof of self-testing

The honest behaviour includes the same correlations as are considered in the CHSH test [CHSH69]. We can thus borrow from previous work [MYS12] on CHSH self-testing, where Theorem 2 is summarized here.

Lemma 9 (McKague et al. [MYS12]). *Given a bipartite state $|\psi'\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ and Hermitian and unitary operators X', Z' on \mathcal{H}_1 and D', E' on \mathcal{H}_2 such that*

$$\langle \psi' | [X'D' - X'E' + Z'D' + Z'E'] | \psi' \rangle \geq 2\sqrt{2} - \epsilon \quad (87)$$

where A and B refer to different subsystems, then

$$\|Z'_A X'_A |\psi'\rangle + X'_A Z'_A |\psi'\rangle\| \leq 2\sqrt{2\sqrt{2}\epsilon} \quad (88)$$

and analogously for the B side.

We can also borrow most of Lemma 7. We must make a small modification in the proof where we use $M'^{X_j}_{k+\frac{n}{2}}$ and $M'^{X_j}_{\ell+\frac{n}{2}}$, since this operator is not defined here. Instead we substitute any question q which has Z in the k th position and X in the $(k + \frac{n}{2})$ th position, and use the operators $M'^q_{k+\frac{n}{2}}$ and $M'^q_{\ell+\frac{n}{2}}$. With this modification we obtain the analogous result to Lemma 7, with the same bounds. Putting everything together, analogously to Theorem 1, we obtain a self-testing result for this strictly parallel test:

Lemma 10. *Given the definitions of operators in section 5.2 if for each $k \in \{1 \dots \frac{n}{2}\}$*

$$\langle \psi' | \left[X'_k \left(D'_{k+\frac{n}{2}} - E'_{k+\frac{n}{2}} \right) + Z'_k \left(D'_{k+\frac{n}{2}} + E'_{k+\frac{n}{2}} \right) \right] | \psi' \rangle \geq 2\sqrt{2} - \epsilon \quad (89)$$

$$\langle \psi' | \left[X'_{k+\frac{n}{2}} (D'_k - E'_k) + Z'_{k+\frac{n}{2}} (D'_k + E'_k) \right] | \psi' \rangle \geq 2\sqrt{2} - \epsilon \quad (90)$$

and for every $q, r \in \{X, Y\}^{\frac{n}{2}}$ and $k \in \{1 \dots \frac{n}{2}\}$ such that $r_{k+\frac{n}{2}}$ is the complement of q_k (i.e., if $q_k = X$ then $q_{k+\frac{n}{2}} = Z$ or vice versa)

$$\langle \psi' | M'^q_k M'^r_{k+\frac{n}{2}} | \psi' \rangle \geq 1 - \epsilon \quad (91)$$

then there exists an isometry Φ and a state $|junk\rangle$ such that for any $p, q \in (0, 1)^n$

$$\begin{aligned} \|\Phi(X'^q Z'^p |\psi'\rangle) - |junk\rangle X^q Z^p |\psi\rangle\| &\leq \sqrt{\sqrt{2}\epsilon \left(\frac{9n^2}{4} + \frac{(3 + 2^{5/4})n}{2} \right)} + \\ &\sqrt{\sqrt{2}\epsilon \left[\frac{9n^2}{8} + n \left(\frac{5|p|}{2} - \frac{1}{4} + \frac{1}{2^{3/4}} \right) + |p| \left(2^{1/4} - \frac{1}{2} \right) \right]}. \end{aligned} \quad (92)$$

We do not need all of the conditions in the lemma, specifically we only need enough questions q and r to make the argument in Lemma 7 work. A subset as used in section 4.

5.4. A non-local game for the new test

The Mayers-Yao test, and our parallel extension of it, are not well suited to being phrased as a non-local game where the referee asks a question and decides to accept or reject based on the answers. The reason is that we have XX and ZZ measurements which should have expected value near zero. So if the referee observes that the measurement outcome is a 1, should the referee accept or reject? The CHSH game, on the other hand, is very straightforward to phrase as a non-local game. In our notation the referee asks Alice either X or Z and Bob either D or E . The referee accepts when Alice's and Bob's answers match, except when the questions are X and E , in which case the

referee accepts when their answers disagree. Our new single e-bit test has two CHSH games as sub-tests (X, Z for Alice, and D, E for Bob, and vice versa) each of which must obey the Cirel'son inequality [Cir80], plus two other questions (X for Alice, Z for Bob and vice versa) where the referee accepts when Alice and Bob's answers agree. It is straightforward to see, then, that the maximum probability of winning the single copy non-local game is

$$\frac{1}{10} \left(2 + 8 \cos \frac{\pi}{8} \right) \quad (93)$$

or in terms of expectation value (where the referee outputs 1 for a win and -1 for a loss), the maximum is

$$\frac{1}{5} \left(2\sqrt{2} + 1 \right). \quad (94)$$

Now, moving to the parallel case, the referee picks questions independently for each sub-test. But what is the winning condition? The referee has lots of data, and has to boil it down to a single bit: accept or reject. There are many ways that the referee could do this. Let us define A_k to be the random variable corresponding to accepting on the k -th sub-test, with 1 meaning accept and -1 meaning reject. The referee will do as follows:

- (i) The referee asks questions independently for each of the $\frac{n}{2}$ sub-tests
- (ii) The referee determines A_k for each sub-test – i.e., whether to accept or reject
- (iii) The referee chooses a number a uniformly at random from $\{-\frac{n}{2} + 1 \dots \frac{n}{2}\}$
- (iv) If $\sum_k A_k \geq a$ the referee accepts, and otherwise rejects

let A be the random variable corresponding to accepting, given the above procedure for the referee, with $A = 1$ being accept and $A = -1$ being reject. Then we have the following lemma:

Lemma 11. *Let $\{A_k\}_{k=1}^m$ be random variables taking values ± 1 . Let A be the random variable defined by the following procedure:*

- (i) Observe $A_1 \dots A_m$
- (ii) Pick a uniformly from $\{-m + 1 \dots m\}$
- (iii) A is given by

$$A = \begin{cases} 1 & \sum_k A_k \geq a \\ -1 & \text{otherwise} \end{cases} \quad (95)$$

Then

$$E(A) = \frac{1}{m} \sum_{k=1}^m E(A_k) \quad (96)$$

Proof. The expectation is given by:

$$E(A) = \frac{1}{2m} \sum_{A_1 \dots A_m} P(A_1 \dots A_m) \sum_a \begin{cases} 1 & \sum_k A_k \geq a \\ -1 & \text{otherwise} \end{cases} \quad (97)$$

Looking at the inner sum for a fixed $A_1 \dots A_m$, when a takes the values $-m+1$ through to $\sum_k A_k$ then the summand is 1. So there are $m + \sum_k A_k$ values of a that will cause the summand to take the value 1, and $m - \sum_k A_k$ that will cause A to take the value -1 . Applying this knowledge to the inner sum we find

$$E(A) = \frac{1}{m} \sum_{A_1 \dots A_m} P(A_1 \dots A_m) \sum_k A_k. \quad (98)$$

Rearranging the order of the sum we get

$$E(A) = \frac{1}{m} \sum_k \sum_{A_1 \dots A_m} P(A_1 \dots A_m) A_k. \quad (99)$$

The inner sum is evidently $E(A_k)$, which finishes the proof. \square

Theorem 2. *Given the definition of A from the preceding discussion, if for some $\delta \geq 0$*

$$E(A) \geq \frac{1}{5} (2\sqrt{2} + 1) - \delta \quad (100)$$

then there exists an isometry Φ and a state $|junk\rangle$ such that for any $p, q \in (0, 1)^n$

$$\begin{aligned} \|\Phi(X'^q Z'^p |\psi'\rangle) - |junk\rangle X^q Z^p |\psi\rangle\| &\leq 10^{\frac{n}{8}} \sqrt{\sqrt{n\delta} \left(\frac{9n^2}{4} + \frac{(3 + 2^{5/4})n}{2} \right)} + \\ &10^{\frac{n}{8}} \sqrt{\sqrt{n\delta} \left[\frac{9n^2}{8} + n \left(\frac{5|p|}{2} - \frac{1}{4} + \frac{1}{2^{3/4}} \right) + |p| \left(2^{1/4} - \frac{1}{2} \right) \right]}. \end{aligned} \quad (101)$$

Proof. Let us introduce some notation to help. The function $f(q, k)$ gives the winning condition for sub-test k given question q . Note that $f(q, k)$ depends only on the k and $k + \frac{n}{2}$ positions of q , i.e., the questions for sub-test k . The expected value for A_k when the question q is asked is then $f(q, k) \langle \psi' | M_k'^q M_{k+\frac{n}{2}}'^q | \psi' \rangle$ and

$$E(A) = \frac{2}{10^{\frac{n}{2}} n} \sum_{q, k} f(q, k) \langle \psi' | M_k'^q M_{k+\frac{n}{2}}'^q | \psi' \rangle \quad (102)$$

where q ranges over the $10^{\frac{n}{2}}$ possible questions. $E(A)$ is bounded above by $\frac{1}{5} (2\sqrt{2} + 1)$ since it is the average of the expectations of k values $E(A_k)$, each of which also has this upper bound.

Now let us estimate the value

$$S := \langle \psi' | \left[X'_k \left(D'_{k+\frac{n}{2}} - E'_{k+\frac{n}{2}} \right) + Z'_k \left(D'_{k+\frac{n}{2}} + E'_{k+\frac{n}{2}} \right) \right] | \psi' \rangle. \quad (103)$$

Clearly $S \leq 2\sqrt{2}$ since this is just CHSH correlations. Note that S is part of the sum making up $E(A)$. Taking the pessimistic view that all other correlations meet their maximum, and that all of the error δ that we see is due to S being smaller than maximum, we find that $S \geq 2\sqrt{2} - \frac{2}{10^{\frac{n}{2}} n} \delta$. A similar argument applies for the A and B sides swapped. Letting

$$\epsilon = \frac{2}{10^{\frac{n}{2}} n} \delta \quad (104)$$

we obtain conditions (89) and (90).

Now for some q, r and k such that $r_{k+\frac{n}{2}}$ is the complement of q_k we look at

$$T := \langle \psi' | M_k'^q M_{k+\frac{n}{2}}'^r | \psi' \rangle. \quad (105)$$

Straightforwardly $T \leq 1$. Again supposing that all other correlations meet their maximum, we find that $T \geq 1 - \epsilon$, giving us (91).

We have established the conditions for Lemma 10, which gives us the desired conclusion. \square

Although we have phrased the non-local game as being strictly parallel, the conditions of Lemma 10 do not need all of the information that a strictly parallel test gives. We can easily define a non-local game using a much smaller set of questions as in Section 4. Much of the above discussion could be adapted to this set of questions, resulting in a non-local game that tests m e-bits using $O(\log m)$ questions and with polynomial scaling in the robustness. We leave the exact details for future work.

We may also modify the referee's processing slightly without changing the basic result. The referee can choose a sub-test k uniformly random and just output A_k . Then $E(A) = \frac{2}{n} \sum_k E(A_k)$, exactly as above.

6. Discussion

We have introduced techniques for performing many self-tests in parallel in the case where we do not have no-signalling restrictions between tests. We gave two constructions which allow for testing many e-bits which are shared between two parties, and we have no other restrictions on the structure of the state or measurements.

Clearly testing in parallel is quite powerful, for example allowing us to test m e-bits using $O(\log m)$ different questions, i.e., $O(\log \log m)$ bits of randomness. An open question is whether adding more questions (for example, all of the questions in a strictly parallel test) can improve the robustness or not. For the strictly parallel non-local game presented here, adding more questions reduces the robustness since we ignore most of the questions and they simply mean that the relevant questions get asked with lower probability.

These results open up many possible directions for future work. Clearly requiring only $O(\log \log m)$ bits of randomness is a remarkable property which could see use in applications. Improving the robustness scaling in the strictly parallel test is also desirable. Of course it should also be possible to apply the same techniques to other self-tests, especially CHSH, allowing them to be used in parallel as well.

Acknowledgements This work is funded by the University of Otago and the Dodd-Walls Centre for Photonic and Quantum Technologies. Thanks to Michael Albert, Valerio Scarani and Carl Miller for valuable feedback.

7. References

- [BLM⁺09] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani. Device-independent state estimation based on Bell’s inequalities. *Physical Review A (Atomic, Molecular, and Optical Physics)*, **80**(6):062327, 2009. DOI:[10.1103/PhysRevA.80.062327](https://doi.org/10.1103/PhysRevA.80.062327). EPRINT [arXiv:0907.2170](https://arxiv.org/abs/0907.2170).
- [CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, **23**(15):880–884, Oct 1969. DOI:[10.1103/PhysRevLett.23.880](https://doi.org/10.1103/PhysRevLett.23.880).
- [Cir80] B. S. Cirel’son. Quantum generalizations of Bell’s inequality. *Letters in Mathematical Physics*, **4**(2):93–100, 03 1980. DOI:[10.1007/BF00417500](https://doi.org/10.1007/BF00417500).
- [McK11] Matthew McKague. Self-testing graph states. In *Proceedings of Theory of Quantum Computation, Communication, and Cryptography*, number 6475 in LNCS, pp. 104–120, October 2011. EPRINT [arXiv:1010.1989](https://arxiv.org/abs/1010.1989).
- [McK13] Matthew McKague. Interactive proofs for BQP via self-tested graph states, September 2013. EPRINT [arxiv:1309.5675](https://arxiv.org/abs/1309.5675).
- [MMMO06] Frédéric Magniez, Dominic Mayers, Michele Mosca, and Harold Ollivier. Self-testing of quantum circuits. In M et al. Bugliesi, editor, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming*, number 4052 in Lecture Notes in Computer Science, pp. 72–83, 2006. DOI:[10.1007/11786986_8](https://doi.org/10.1007/11786986_8). EPRINT [arXiv:quant-ph/0512111v1](https://arxiv.org/abs/quant-ph/0512111v1).
- [MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Information and Computation*, **4**(4):273–286, July 2004. EPRINT [arXiv:quant-ph/0307205](https://arxiv.org/abs/quant-ph/0307205).
- [MYS12] M McKague, T H Yang, and V Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, **45**(45):455304, 2012. DOI:[10.1088/1751-8113/45/45/455304](https://doi.org/10.1088/1751-8113/45/45/455304). EPRINT [arXiv:1203.2976](https://arxiv.org/abs/1203.2976).
- [PR92] Sandu Popescu and Daniel Rohrlich. Which states violate Bell’s inequality maximally? *Physics Letters A*, **169**(6):411 – 414, 1992. DOI:[10.1016/0375-9601\(92\)90819-8](https://doi.org/10.1016/0375-9601(92)90819-8).
- [RUV13] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, **496**(7446):456–460, 04 2013. DOI:[10.1038/nature12035](https://doi.org/10.1038/nature12035).
- [WBMS15] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent self-testing of two singlets. *In preparation*, 2015.